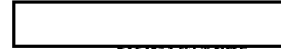


SECRET



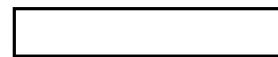
25X1

SECURITY
1957

MANUAL FOR SECURITY OF
INFORMATION AND MATERIAL

SECRET

SECRET



25X1

SECRET

Draft A 1957

FOREWORD

This handbook sets forth the security provisions for protecting classified information and material.

DISTRIBUTION: AB

Job #2019-A-BMT

SECRET

**MANUAL FOR SECURITY OF
INFORMATION AND MATERIAL**

Par.

Page

**CHAPTER I: STATUTORY REQUIREMENTS FOR CARE AND USE OF
OFFICIAL DATA**

1. U.S.C., TITLE 18, SECTION 793
2. U.S.C., TITLE 18, SECTION 794
3. U.S.C., TITLE 18, TEMPORARY EXTENSION OF SECTION 794

CHAPTER II: CLASSIFICATION OF OFFICIAL INFORMATION AND MATERIAL

4. DEFINITIONS
5. CLASSIFICATION CONTROL NETWORK
6. CLASSIFICATION CATEGORIES
7. ASSIGNMENT OF CLASSIFICATION CATEGORIES
8. CLASSIFICATION MARKING
9. RECLASSIFICATION AND DECLASSIFICATION PROCEDURE

CHAPTER III: CONTROL-Stamping OF INFORMATION OR MATERIAL

10. TYPES OF CONTROL STAMPS
11. CONTROL-STAMP MARKING

CHAPTER IV: CONTROL OF PERSONNEL-SECURITY FILES

12. DEFINITIONS
13. CONTROL REQUIREMENTS
14. PROCEDURES FOR RELEASE OF PERSONNEL-SECURITY INFORMATION

CHAPTER V: CONTROL OF NSC INFORMATION AND MATERIAL

15. CONTROL SYSTEM
16. CONTROL PROCEDURES

**CHAPTER VI: CONTROL OF STAFF CRYPTOGRAPHIC INFORMATION
AND MATERIAL**

17. HANDLING
18. CUSTODIANS

**CHAPTER VII: PROCEDURES FOR PROTECTION OF CLASSIFIED AND
CONTROLLED INFORMATION OR MATERIAL**

19. STORAGE
20. TRANSMISSION
21. REPRODUCTION
22. DESTRUCTION

CHAPTER VIII: CONTROL OF AEC RESTRICTED DATA

23. DEFINITION

25X2

SECRET

CHAPTER I: STATUTORY REQUIREMENTS FOR CARE AND USE OF OFFICIAL DATA

Par.

Page

1. U.S.C., TITLE 18, SECTION 793
2. U.S.C., TITLE 18, SECTION 794
3. U.S.C., TITLE 18, TEMPORARY EXTENSION OF SECTION 794

SECRET

SECRET

CHAPTER I: STATUTORY REQUIREMENTS FOR CARE AND USE OF OFFICIAL DATA

This chapter contains extracts from statutes pertaining to espionage. These statutes state the principles governing the care and use of official data and prescribe penalties of imprisonment or death for violation of such principles. Under the provisions of Public Law 99, 83rd Congress (18 U.S.C. 798), the wartime penalties for espionage are in effect until six months after the termination of the present emergency, or until such earlier date as may be prescribed by Congress. These extracts were taken from the United States Code, as indicated below:

1. United States Code, Title 18, Crime and Criminal Procedure: "Section 793. Gathering, transmitting, or losing defense information
"(a) Whoever, for the purpose of obtaining information respecting the national defense with intent or reason to believe that the information is to be used to the injury of the United States, or to the advantage of any foreign nation, goes upon, enters, flies over, or otherwise obtains information concerning any vessel, aircraft, work of defense, navy yard, naval station, submarine base, fueling station, fort, battery, torpedo station, dockyard, canal, railroad, arsenal, camp, factory, mine, telegraph, telephone, wireless, or signal station, building, office, research laboratory or station or other place connected with the national defense owned or constructed, or in progress of construction by the

SECRET

SECRET

STATUTORY REQUIREMENTS FOR CARE AND USE OF OFFICIAL DATA

- United States or under the control of the United States, or of any of its officers, departments, or agencies, or within the exclusive jurisdiction of the United States, or any place in which any vessel, aircraft, arms, munitions, or other materials or instruments for use in time of war are being made, prepared, repaired, stored, or are the subject of research or development, under any contract or agreement with the United States, or any department or agency thereof, or with any person on behalf of the United States, or otherwise on behalf of the United States, or any prohibited place so designated by the President by proclamation in time of war or in case of national emergency in which anything for the use of the Army, Navy, or Air Force is being prepared or constructed or stored, information as to which prohibited place the President has determined would be prejudicial to the national defense; or
- "(b) Whoever, for the purpose aforesaid, and with like intent or reason to believe, copies, takes, makes, or obtains, or attempts to copy, take, make, or obtain, any sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, document, writing, or note of anything connected with the national defense; or
- "(c) Whoever, for the purpose aforesaid, receives or obtains or agrees or attempts to receive or obtain from any person, or from any source whatever, any document, writing, code book, signal book,

SECRET

~~SECRET~~

STATUTORY REQUIREMENTS FOR CARE AND USE OF OFFICIAL DATA

sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note, or anything connected with the national defense, knowing or having reason to believe, at the time he receives or obtains, or agrees or attempts to receive or obtain it, that it has been or will be obtained, taken, made, or disposed of by any person contrary to the provisions of this chapter; or

"(d) Whoever, lawfully having possession of, access to, control over, or being entrusted with any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted or attempts to communicate, deliver, transmit or cause to be communicated, delivered or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it on demand to the officer or employee of the United States entitled to receive it; or

"(e) Whoever having unauthorized possession of, access to, or control over any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model,

81187 3

~~SECRET~~

SECRET

STATUTORY REQUIREMENTS FOR CARE AND USE OF OFFICIAL DATA

instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it; or

"(f) Whoever, being entrusted with or having lawful possession or control of any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, note, or information, relating to the national defense, (1) through gross negligence permits the same to be removed from its proper place of custody or delivered to anyone in violation of his trust, or to be lost, stolen, abstracted, or destroyed, or (2) having knowledge that the same has been illegally removed from its proper place of custody or delivered to anyone in violation of his trust, or lost or stolen, abstracted, or destroyed, and fails to make prompt report of such loss, theft, abstraction, or destruction to his superior officer --

SECRET

STATUTORY REQUIREMENTS FOR CARE AND USE OF OFFICIAL DATA

Shall be fined not more than \$10,000 or imprisoned not more than ten years, or both.

"(g) If two or more persons conspire to violate any of the foregoing provisions of this section, and one or more of such persons do any act to effect the object of the conspiracy, each of the parties to such conspiracy shall be subject to the punishment provided for the offense which is the object of such conspiracy. (June 25, 1948, c. 445, Section 1, 62 Stat. 736, amended Sept. 23, 1950, c. 1024, Section 18, 64 Stat. 1003)."

2. United States Code, Title 18, Crime and Criminal Procedure: "Section 794. Gathering or delivering defense information to aid foreign government

"(a) Whoever, with intent or reason to believe that it is to be used to the injury of the United States or to the advantage of a foreign nation, communicates, delivers, or transmits, or attempts to communicate, deliver, or transmit, to any foreign government, or to any faction or party or military or naval force within a foreign country, whether recognized or unrecognized by the United States, or to any representative, officer, agent, employee, subject, or citizen thereof, either directly or indirectly, any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, note, instrument, appliance, or information relating to the national defense,

SECRET

SECRET

STATUTORY REQUIREMENTS FOR CARE AND USE OF OFFICIAL DATA

shall be punished by death or by imprisonment for any term of years or for life.

"(b) Whoever, in time of war, with intent that the same shall be communicated to the enemy, collects, records, publishes, or communicates, or attempts to elicit any information with respect to the movement, numbers, description, condition, or disposition, of any of the Armed Forces, ships, aircraft, or war materials of the United States, or with respect to the plans or conduct or supposed plans or conduct of any naval or military operations, or with respect to any works or measures undertaken for or connected with, or intended for the fortification or defense of any place, or any other information relating to the public defense, which might be useful to the enemy, shall be punished by death or by imprisonment for any term of years or for life.

"(c) If two or more persons conspire to violate this section, and one or more of such persons do any act to effect the object of the conspiracy, each of the parties to such conspiracy shall be subject to the punishment provided for the offense which is the object of such conspiracy. (As amended September 3, 1954, Ch. 1261, Title II, Section 201, 68 Stat. 1219)."

3. United States Code, Title 18, Crimes and Criminal Procedure: "Section 798. Temporary extension of section 794.

SECRET

SECRET

STATUTORY REQUIREMENTS FOR CARE AND USE OF OFFICIAL DATA

"The provisions of section 794 of this title, as amended and extended by section 1(a)(29) of the Emergency Powers Continuation Act (66 Stat. 333), as further amended by Public Law 12, Eighty-third Congress, in addition to coming into full force and effect in time of war shall remain in full force and effect until six months after the termination of the national emergency proclaimed by the President on December 16, 1950 (Proc. 2912, 3 C.F.R., 1950 Supp., p. 71), or such earlier date as may be prescribed by concurrent resolution of the Congress, and acts which would give rise to legal consequences and penalties under section 794 when performed during a state of war shall give rise to the same legal consequences and penalties when they are performed during the period above provided for. (Added June 30, 1953, c. 175, section 4, 67 Stat. 133.)"

SECRET

SECRET

CHAPTER II: CLASSIFICATION OF OFFICIAL INFORMATION AND MATERIAL

Par.

Page

4. DEFINITIONS
5. CLASSIFICATION CONTROL NETWORK
6. CLASSIFICATION CATEGORIES
7. ASSIGNMENT OF CLASSIFICATION CATEGORIES
8. CLASSIFICATION MARKING
9. RECLASSIFICATION AND DECLASSIFICATION PROCEDURE

SECRET

SECRET

CHAPTER II: CLASSIFICATION OF OFFICIAL INFORMATION AND MATERIAL

4. DEFINITIONS

a. SECURITY CLASSIFICATION

"Security classification," hereinafter referred to as "classification," is the degree of secrecy that is warranted to insure protection of information and material.

The determination of the degree of secrecy is based upon the consideration of such information or material in relation to the potential effect its disclosure might have on the defense of the nation or on intelligence efforts of CIA or the IAC Agencies. Information and material shall be classified in descending order of importance as Top Secret, Secret, or Confidential.

b. COMPROMISE

"Compromise" is the known or suspected exposure of classified information or material to an unauthorized person and the loss of security which results therefrom.

c. DECLASSIFICATION

"Declassification" is the considered, authorized removal of a classification from classified information or material.

d. RECLASSIFICATION

"Reclassification" is the considered, authorized removal of a classification from information or material and the immediate assignment of a more appropriate classification.

e. DOWNGRADING

SECRET

SECRET

CLASSIFICATION OF OFFICIAL INFORMATION AND MATERIAL

"Downgrading" is the considered, authorized removal of a classification from information or material and the immediate assignment of a lower classification.

f. UPGRADING

"Upgrading" is the considered, authorized removal of a classification from information or material and the immediate assignment of a higher classification.

5. CLASSIFICATION CONTROL SYSTEM

- a. The CIA Classification Control System, established by the Assistant Director for Central Reference in order to control the classification of information or material and to insure its protection against unauthorized disclosure, shall consist of:
- (1) The CIA Classification Control Officer designated by the Assistant Director for Central Reference,
 - (2) Assistant Classification Control Officers who are key personnel designated by Deputy Directors and Operating Officials, and
 - (3) Authorized Classifiers designated by Assistant Classification Control Officers.
- b. The CIA Classification Control Officer shall be responsible for the administration and technical supervision of the Classification Control System.
- c. Deputy Directors and Operating Officials shall designate as many Assistant Classification Control Officers within their respective

9
SECRET

SECRET

CLASSIFICATION OF OFFICIAL INFORMATION AND MATERIAL

areas of jurisdiction as may be necessary for the effective administration and supervision of classification procedures and activities. They shall notify the CIA Classification Control Officer in writing of the names and titles of all individuals so designated, and of the effective date of the designation and any subsequent changes thereto immediately upon making such designations or changes.

- d. Assistant Classification Control Officers shall designate as many Authorized Classifiers as may be necessary for the effective application of classification procedures within their respective areas of jurisdiction.
- e. Deputy Directors and Operating Officials shall designate persons to be responsible for the continuing review of classified information and material for the purpose of declassifying or reclassifying. Assistant Classification Control Officers and Authorized Classifiers should be assigned this responsibility in addition to their other duties; but, where this is not practicable, other persons may be designated for this purpose.

6. CLASSIFICATION CATEGORIES

Information and material shall be classified in accordance with the following definitions of classification categories as set forth in this manual. Material will not be given a higher classification than is justifiable on the basis of content.

- a. TOP SECRET

SECRET

SECRET

CLASSIFICATION OF OFFICIAL INFORMATION AND MATERIAL

The classification TOP SECRET shall be authorized only for information or material which requires the highest degree of protection. The Top Secret classification shall be applied only to that information or material, the defense aspect of which is paramount, and the unauthorized disclosure of which could result in EXCEPTIONALLY GRAVE damage to the nation such as leading to a definite break in diplomatic relations affecting the defense of the United States, or armed attack against the United States or its allies, a war, or the compromise of military or defense plans, or intelligence operations, or scientific or technological developments vital to the national defense. EXCEPTIONALLY GRAVE damage to the nation may be caused where any one or all of the foregoing conditions could result from the compromise of information or material of any one or more of the following or similar types:

- (1) War plans, plans or particulars of future major or special operations of war, and particulars of important dispositions of our forces related directly thereto; or
- (2) Intelligence documents and information contained therein that reveal a major intelligence effort on the part of the United States, which could permit the identification of a clandestine agent or agents, or which could permit an evaluation by unauthorized persons of the success obtained by, or the capabilities of, our intelligence services; or
- (3) Information regarding radically new and extremely important equipment or munitions of war; or

SECRET

SECRET

CLASSIFICATION OF OFFICIAL INFORMATION AND MATERIAL

- (4) Information regarding extremely significant political or economic policies of or conditions in the United States, or involving relationships of the United States with another country or countries; or
- (5) Photographs, negatives, photostats, diagrams, models, or other reproductions or replicas of Top Secret information or material.

b. **SECRET**

The classification **SECRET** shall be applied to information or material, the unauthorized disclosure of which could result in **SERIOUS** damage to the nation or its defense. Information and material shall be classified **SECRET** if its unauthorized disclosure could jeopardize the international relations of the United States; endanger the effectiveness of a program or policy of vital importance to the national defense; result in the compromise of important military or defense plans or scientific or technological developments important to the national defense; reveal important intelligence operations; or which could be of advantage to a foreign nation in enabling it to cause serious injury to the national defense or intelligence effort of the United States. Serious damage to the nation may be caused where any one or all of the foregoing conditions could result from the compromise of information or material of any one or more of the following or similar types:

- (1) Particulars regarding plans for operations or projects and active operations and projects of this Agency; or

SECRET

SECRET

CLASSIFICATION OF OFFICIAL INFORMATION AND MATERIAL

- (2) Important improvements to existing, and the development of new munitions of war including scientific and technical developments related thereto; or
- (3) Information or material concerning specific quantities of war reserves; or
- (4) Information or material of any kind possessed by the Agency where knowledge of CIA possession of such information or material could itself be of significant potential value to a foreign country; or
- (5) Information or material relating to military defenses; the strength of United States or allied armed forces or the identity, composition, or location of units, etc; or
- (6) Adverse reports regarding the general morale of major United States operations; or
- (7) Photographs, negatives, photostats, diagrams, models, or other reproductions or replicas of secret information or material.

c. CONFIDENTIAL

The classification CONFIDENTIAL shall be applied to information or material, the unauthorized disclosure of which could be PREJUDICIAL to the defense interests or intelligence activities of the nation. Several examples of the types of information or material which should be classified CONFIDENTIAL are set forth below:

- (1) Routine intelligence, operational or battle reports that contain information of value but not of vital interest to a foreign nation; or

SECRET

SECRET

CLASSIFICATION OF OFFICIAL INFORMATION AND MATERIAL

- (2) Military radio frequency allocations and call-sign assignments of special significance; or
 - (3) Information which indicates strength of United States military forces, or quantity of specific items of equipment pertaining thereto; or
 - (4) Technical documents and manuals used for training, maintenance, or inspection of important new equipment or munitions of war; or
 - (5) Information regarding the content of reports of investigations, and documents of an intelligence nature which could be of value but not of vital interest to a foreign country; or
 - (6) Technical research information regarding processes of manufacture, or the design and development of new material that may be of a distinct military asset, but not a matter of general knowledge; or
 - (7) Information and records regarding industrial mobilization compiled in defense planning; or
 - (8) Photographs, negatives, photostats, diagrams, models, or other reproductions, replicas, or facsimiles of confidential information or material.
7. ASSIGNMENT OF CLASSIFICATION CATEGORIES
- a. All information and material shall be carefully considered in terms of the potential effect its unauthorized disclosure might have on the defense or intelligence effort of the nation, and shall be classified accordingly.
 - b. Every individual employed by, assigned to, or associated with this Agency shall be personally responsible for the deliberate consideration

SECRET

SECRET

CLASSIFICATION OF OFFICIAL INFORMATION AND MATERIAL

of official information and material that he originates and for recommending the appropriate classification. This recommended classification shall be subject to review and approval by an individual who is an Assistant Classification Control Officer or an Authorized Classifier in the component of the originator.

- c. When the interests of two or more Agency components are involved in the classification, reclassification, or declassification of information or material, and the issue cannot be resolved to the satisfaction of the parties involved, it shall be submitted to the CIA Classification Control Officer for resolution.
- d. Each document, including extracts and excerpts, shall be classified on the basis of its own content, and not necessarily according to its relationship to other documents. Any document, however, referring to or relating to other classified documents shall be carefully scrutinized to insure that the classification assigned will not jeopardize those related documents that have been given a higher classification.
- e. Reference to classified information or material shall not be classified when the reference does not in itself reveal the substance of that material.
- f. A document, product, or substance shall bear a classification at least as high as that of its highest classified parts. The document, product, or substance shall bear only one overall classification, even though pages, paragraphs, sections, or parts thereof bear different classifications or no classification.

SECRET

SECRET

CLASSIFICATION OF OFFICIAL INFORMATION AND MATERIAL

- g. The classification of a file, or a group of physically connected documents, or material shall be at least as high as the classification of the most highly classified document contained therein. Documents or materials separated from the file or group shall be handled in accordance with the individual classification assigned to each.
- h. A transmittal letter or memorandum shall be classified at least as high as its highest classified enclosure or attachment.
- i. Classified information or material originated by a foreign government and furnished to this Agency by that government shall be assigned a classification that will assure a degree of protection equivalent to or greater than that required by the originating government.
- j. At the time of original classification, consideration shall be given to an automatic change in classification after a specified date or the occurrence of a specified event, or upon removal of classified enclosures. Where appropriate, such material will be marked in accordance with paragraph 9.b.(1) below.
- k. When classified information or material is furnished to authorized persons outside CIA, the following notation (Espionage Stamp) will be placed on the material, in addition to the classification:

"This material contains information affecting the national defense of the United States within the meaning of the espionage laws, Title 18, USC, Secs. 793 and 794, the transmission or revelation of which in any manner to an unauthorized person is prohibited by law."

8. CLASSIFICATION MARKING

SECRET

SECRET

CLASSIFICATION OF OFFICIAL INFORMATION AND MATERIAL

a. GENERAL

- (1) Unclassified information or material shall be marked or stamped UNCLASSIFIED only when it is essential to convey to a recipient that it has been examined specifically with a view to assigning a classification and a positive determination has been made that it should be unclassified.
- (2) The assigned classification on unbound documents such as letters, memorandums, reports, and other similar documents, the pages of which are not permanently and securely fastened together, shall be conspicuously marked in ^{bold} capital letters noticeably larger ^{and bolder} than the print of the text, at the top and bottom of each page, so that the marking will be clearly visible when the pages are clipped or stapled together. The original and all copies of the finished document and all rough drafts and notes shall be marked with the appropriate classification.
- (3) The classification of bound documents with the pages permanently and securely fastened together shall, as a minimum, be conspicuously marked on the outside of the front cover, on the title page, on the first page, on the back page, and on the outside of the back cover. In each case the markings shall be applied to the top and bottom of the page or cover. Bound documents are books or pamphlets, the pages of which are permanently and securely fastened together so that one or more pages cannot be extracted from the bound copy without defacement or alteration

SECRET

~~SECRET~~

CLASSIFICATION OF OFFICIAL INFORMATION AND MATERIAL

of the book. The foregoing minimum requirement for classification marking of bound documents does not preclude the classification of each page when it is considered desirable by the Authorized Classifier.

- (4) The classification of charts, maps, and drawings shall be marked under the legend, title block, or scale in such a manner that such classification will be reproduced on all copies; in addition, the classification shall also be marked at the top and bottom of such charts, maps and drawings.
- (5) The classification of photographs, films, recordings, and their containers shall be marked conspicuously.
- (6) The classification of special equipment, bulk material, or shipments shall be marked in the manner that is most consistent with the character of the material and the operations involved. In special cases, security conditions will require that the classification NOT appear on the material that, because of its nature or construction, cannot be kept from general or undesirable observation. In such cases, classification marking may in itself constitute a hazard to security.

b. METHODS OF MARKING

- (1) The classification TOP SECRET is the only classification that may be preprinted on blank paper. Requests to preprint other classifications require the approval of the CIA Classification Control Officer.

~~SECRET~~

SECRET

CLASSIFICATION OF OFFICIAL INFORMATION AND MATERIAL

- (2) The classification of documents shall be marked in red by use of a rubber stamp, stencil, classification plate, or other appropriate means, except manuscripts prepared for photographic reproduction. *red is a limiting factor.* In such instances the classification shall be marked in black or other color suitable for photographic reproduction. *process to be used.*
- (3) Printed documents, including charts, maps, and drawings, shall bear the appropriate classification in type that is conspicuously *both* larger than the type used to reproduce the text of the document. *substantive different*
- (4) The classification of information to be reproduced from stencils, ditto-masters, *direct image offset masters* duplimate, or other similar media may be typed onto the master in all capital letters and hyphenated, i.e., S-E-C-R-E-T or C-O-N-F-I-D-E-N-T-I-A-L.
- (5) The preclassification of printed forms necessitates the application of prescribed security measures for the handling and safe-keeping of such forms as classified documents. In many cases, however, the printed information on the blank forms does not warrant a classification. To avoid needless security measures, blank forms not inherently classifiable as CONFIDENTIAL or higher shall be printed with the words "when filled in" below the classification considered appropriate to the form when it is filled in. Accordingly, forms so identified are merely unclassified documents until entries are made. Forms not so

SECRET

SECRET

CLASSIFICATION OF OFFICIAL INFORMATION AND MATERIAL

identified must be assumed to be classified as indicated thereon, and protected accordingly. If a blank form is not inherently classifiable but should, nevertheless, not be handled as unclassified material because of the information contained thereon, an appropriate control statement shall be used to indicate that the form merits special handling in accordance with appropriate storage requirements. ILLEGIB

9. RECLASSIFICATION AND DECLASSIFICATION PROCEDURES

a. GENERAL

Where practicable, notification shall be given to all recipients of classified information or material that has been reclassified or declassified, in order to preserve the effectiveness and integrity of the classification system and to reduce the accumulation of classified material that no longer requires the original classification.

b. REQUIREMENTS FOR CHANGING CLASSIFICATION

The following requirements shall be observed for changes in classification:

(1) Automatic Changes in Classification

As far as practicable, the Assistant Classification Control Officer or Authorized Classifier shall indicate on information or material at the time of original classification that after a specified event or date, or upon removal of classified enclosures, the information or material shall be downgraded or declassified.

SECRET

SECRET

CLASSIFICATION OF OFFICIAL INFORMATION AND MATERIAL

This statement may be placed on information or material by means of a rubber stamp or typing. On documents it shall be placed on the cover sheet or first page. Examples:

"This document is considered to be unclassified (or downgraded to _____) three (3) months following the conclusion of the operation."

"This document will be considered unclassified (or downgraded to _____) upon removal of the enclosures."

(2) Nonautomatic Changes in Classifications

Assistant Classification Control Officers, Authorized Classifiers or other persons designated by Deputy Directors or Operating Officials to review classified information and material, may downgrade or declassify such material when circumstances no longer warrant its retention in its original classification, provided the consent of the original classifying authority has been obtained. Deputy Directors and Operating Officials having primary cognizance over the subject matter involved may change a classification that has been assigned by the originator in an Agency field installation or declassify when such action is deemed appropriate without reference to the original classifying authority. Classified information or material originated outside of the Agency, in other departments and agencies of the government, shall not be reclassified or declassified without written authority from the originator. Extracts from or paraphrases of

SECRET

SECRET

CLASSIFICATION OF OFFICIAL INFORMATION AND MATERIAL

classified documents shall also require the consent of the original classifying authority for downgrading or declassification unless the office or staff making such an extract knows positively that the document warrants a classification lower than that of the document from which it was extracted, or that it does not contain classified matter.

c. MARKING

(1) Changes in Classification

Whenever classified information or material is declassified or reclassified by other than automatic authority as described in paragraph 9 above, such material shall be marked or stamped in a prominent place to state in effect:

CENTRAL INTELLIGENCE AGENCY

CLASSIFICATION

Canceled
Change to _____

BY AUTHORITY OF

Name _____
Office _____
Date _____

Rubber stamps for this purpose may be obtained from the appropriate Building Supply Officer. In addition, the old classification shall be stricken out and the new classification stated in accordance with the requirements set forth herein. When such reclassification or declassification occurs as a result

SECRET

SECRET

CLASSIFICATION OF OFFICIAL INFORMATION AND MATERIAL

of notification from the Assistant Director for Central Reference, the number of such notification should be indicated near his signature.

d. DOWNGRADING AND UPGRADING

When a Top Secret document is downgraded or declassified it shall be stamped with the information and authority appearing above and Form No. 26, Signature Record and Cover Sheet (~~redesignated from Form No. 38-13~~), shall be completed and forwarded to the CIA Top Secret Control Officer in the Office of Central Reference.

If the recipient or custodian of classified information or material believes that it warrants a higher classification, such material shall be protected in accordance with the classification deemed appropriate and a request made to the appropriate Assistant Classification Control Officer, or Authorized Classifier, who shall upgrade the present classification after he obtains the consent of the original classifying authority. These requirements are applicable to material received in CIA from other departments or agencies of the Government as well as to information and material of CIA origin.

e. NOTIFICATION OF CHANGE IN CLASSIFICATION

Where practicable, notification given to recipients of classified information or material when the classification has been changed, shall include the following information:

- (1) CIA document control number
- (2) Other identification or control number
- (3) Date of document
- (4) Title or subject

SECRET

SECRET

CLASSIFICATION OF OFFICIAL INFORMATION AND MATERIAL

(5) Name of originating agency or department

(6) Reclassification or declassification action

The Assistant Director for Central Reference shall issue periodic notices to other Government agencies and departments receiving CIA classified information or material on which the classification has been changed or canceled. Notification shall also be given by the Director of Central Reference on CIA information or material which has been circulated within CIA and on which the classification has been changed or canceled. This subparagraph shall apply only to information or material that has been collected and disseminated through the Office of Central Reference.

f. INFORMATION AND MATERIAL OFFICIALLY TRANSFERRED BETWEEN GOVERNMENT AGENCIES OR DEPARTMENTS

When classified information or material is transferred by or pursuant to statute or Executive order to CIA from another Government agency or department for use as a part of this Agency's official files or property, as distinguished from transfers for purposes of storage, CIA shall be deemed to be the "appropriate classifying authority" for all purposes under this manual, including reclassification or declassification. The provisions set forth in this paragraph and in Section 4 (c) of Executive Order 10501 dated November 5, 1953 are also applicable to classified information or material transferred by statute or Executive order from CIA to another agency or department of the Government.

SECRET

CHAPTER III: CONTROL-STAMPING OF INFORMATION OR MATERIAL

10. TYPES OF CONTROL STAMPS

- a. The standardization of stamps and procedures set forth herein does not preclude the addition of those internal controls considered essential to meet extraordinary internal requirements.
- b. These stamps and procedures, as set forth in DCID 11/2, do not affect the special controls over the dissemination and use of special and atomic intelligence; information subject to copyright, libel, slander and communication laws; information which for moral, ethical or legal information must be protected; or unclassified information or material published for non-governmental use.
- c. Whenever it is deemed necessary to provide for control of intelligence or information, in addition to the protection provided by a security classification, the appropriate control stamp or stamps will be placed (preferably underneath the security classification) upon a document and may be followed by the appropriate definition below or used alone. The control stamps, described in paragraphs (1) through (7) below, will be placed only upon classified information or material. Stamps will be in full capital letters.

(1) NOT RELEASABLE TO FOREIGN NATIONALS

Dissemination limited to United States officials. No dissemination of this material will be made to foreign nationals and immigrant aliens, including U. S. Government employed, utilized, or integrated foreign nationals and immigrant aliens, without permission of the originating agency, except as specified in

25X1

SECRET

CONTROL-STAMPING OF INFORMATION OR MATERIAL

- (a) The originating agency may abbreviate this stamp to NOFORN.
 - (b) When the originating agency permits the release of any of its information or materials to certain foreign nationals and immigrant aliens, it will modify this stamp, e.g., by adding or other clear and appropriate modification.
 - (c) The absence of this stamp on classified information or material does not mean that the receiving agency may disseminate such material to foreign nationals and immigrant aliens without permission of the originating agency.
- (2) NO DISSEM ABROAD
- Dissemination limited to the continental United States exclusive of territories and possessions, unless permission of the originating agency is obtained.
- (3) NATIONAL SECURITY COUNCIL PARTICIPATING AGENCIES ONLY
- Dissemination limited to the Bureau of the Budget, International Cooperation Administration, Department of the Treasury, Office of Defense Mobilization, staff of the Operations Coordinating Board, Federal Civil Defense Administration, all components of the Departments of Defense and State, the Atomic Energy Commission, Federal Bureau of Investigation, and Central Intelligence Agency, unless permission of the originating agency is obtained.
- (4) INTELL COMPONENTS ONLY

25X1

SECRET

SECRET

CONTROL-STAMPING OF INFORMATION OR MATERIAL

Dissemination limited to CIA, AEC, and FBI; and, within State and Defense, to the intelligence components, other offices producing NIS elements, and higher echelons with their immediate supporting staff, unless permission of the originating agency is obtained.

(5) LIMITED

Dissemination limited to full-time employees of CIA, AEC and FBI; and, within State and Defense, to the intelligence components, other offices producing NIS elements, and higher echelons with their immediate supporting staffs. Not to be disseminated to consultants, external projects or reserve personnel on short-term active duty (excepting individuals who are normally full-time employees of CIA, AEC, FBI, State or Defense) unless the written permission of the originating agency is obtained.

(6) CONTINUED CONTROL

Information may be used in only that finished intelligence which bears the same controls as the information itself.

(7) BACKGROUND USE ONLY

Information bearing this stamp will not be included in any intelligence publication without permission of the originating agency.

(8) CIA INTERNAL USE ONLY

This is a control stamp for information which, if disclosed, would violate existing Agency policy regarding protection of

SECRET

SECRET**CONTROL-STAMPING OF INFORMATION OR MATERIAL**

sources and methods. It may be used alone or in conjunction with a defense classification. Intelligence or information so marked may not be released or shown to anyone outside the Agency without permission of the originating office. Within the Agency, intelligence or information so marked may be released only to full-time Agency officers and employees and is not to be disseminated to consultants, external projects, or reserve personnel on short-term active duty unless permission of the originating office is obtained.

(9) FOR OFFICIAL USE ONLY

This control stamp may be used whenever intelligence or information does not warrant a defense classification, but does require some dissemination limitation. Intelligence or information bearing this stamp may be used for official purposes by foreign governments which have been authorized to receive it by the originating agency. This information may be disclosed to non-Governmental persons and organizations only with permission of the originating agency. This control stamp is used alone and never in conjunction with a defense classification.

11. CONTROL-STAMP MARKING**a. MARKING DOCUMENTS**

Documents will be marked with control stamps in full capitals ~~immediately~~ ^{immediately} below the security-classification marking. When the control stamp is used without a security classification (i.e., either of the

SECRET

SECRET

CONTROL-STAMPING OF INFORMATION OR MATERIAL

stamps described in subparagraphs (8) and (9) above), such marking will be made in the manner required for a security classification (see paragraph 9 above).

b. **MULTIPLE-CONTROL STAMPS**

ILLEGIB

If a document warrants the application of more than one control stamp, such stamps will be placed on a single line beneath the classification, and separated by a diagonal line (i.e., NOFORN/LIMITED/CONTINUED CONTROL). When the publication is composed of several separate items, each item shall be marked with the appropriate classification control and/or stamp or stamps (i.e., SECRET/NOFORN/CONTINUED CONTROL, or SECRET/LIMITED) in which case the overall publication must be marked with a classification and control stamp to protect any item, i.e.

SECRET
NOFORN/LIMITED/CONTINUED CONTROL

c. **REMOVAL OR MODIFICATION OF CONTROL STAMPS**

Where the originating agency has determined that a control stamp is no longer needed, indication of such change may be made by marking through the control stamp, or where the control stamp is NOFORN and release has been authorized to a foreign government, the words "Except _____" indicating the name of the country may be added to the document.

SECRET

SECRET

CHAPTER IV: CONTROL OF PERSONNEL-SECURITY FILES

Par.

Page

12. DEFINITIONS

13. CONTROL REQUIREMENTS

14. PROCEDURES FOR RELEASE OF PERSONNEL-SECURITY INFORMATION

SECRET

12. DEFINITIONS

a. PERSONNEL SECURITY FILES

"Personnel security files" are those held in the custody of the Director of Security and contain information pertaining to the loyalty or security of CIA employees or persons of interest to CIA.

b. INVESTIGATIVE INFORMATION

"Investigative information" is limited to information that has been obtained (or is obtainable) by means of a security investigation.

13. CONTROL REQUIREMENTS

a. Personnel of the Agency who are authorized to handle personnel security files and records, as part of their regular assigned duties, shall not inspect or review such files and records except on a definite need-to-know basis in the course of official business and shall exercise the utmost care in preventing unauthorized persons from gaining access to their contents.

b. Any questions concerning the application of control requirements of personnel security files and records will be referred to the Director of Security for decision or appropriate action. In making his decision or taking action, the Director of Security shall be responsible for protecting the confidential character and sources of such information.

14. PROCEDURES FOR RELEASE OF PERSONNEL-SECURITY INFORMATION

a. WITHIN CIA

(1) Personnel security files and records authorized for release shall be hand-carried by a representative of the Director of Security

SECRET

CONTROL OF PERSONNEL-SECURITY FILES

and delivered personally to the individual who has been authorized to review the files or records. In returning such material to the Office of Security, the individual who has been authorized to review it will either deliver it personally or have it hand-carried by a representative of the Director of Security.

- (2) Under no circumstances shall personnel security information be transmitted through the regular mail channels of the Agency.

b. OUTSIDE OF CIA

- (1) The Director of Security, in releasing investigative data to representatives of agencies and departments of the executive branch of the Government, will insure that such representatives have been accredited to CIA, and that they possess authentic credentials from their parent agency or department.
- (2) The accredited representative may abstract, in whole or in part, the information that is released to him, after he has signed a pledge that he will not reveal the source of the information to unauthorized persons.

SECRET

SECRET

CHAPTER V: CONTROL OF NSC INFORMATION AND MATERIAL

Par.

Page

15. CONTROL SYSTEM

16. CONTROL PROCEDURES

SECRET

SECRET

SECRET

CHAPTER V: CONTROL OF NSC INFORMATION AND MATERIAL

15. CONTROL SYSTEM

- a. In addition to the normal requirements applicable to the control of any Top Secret document, by direction of the President, a special control system is established in the Agency for handling of all Top Secret NSC documents. This involves the use of an NSC Top Secret numbering system. For the purpose of this control system classified NSC information will be considered to include classified information contained in documents issued by the NSC Secretariat and documents originating in CIA for transmittal to the NSC Secretariat and all classified information discussed at all meetings of the NSC, the NSC Planning Board, and the NSC Planning Board Assistants.
- b. EXCEPTIONS

Specific documents or categories of documents may be excepted from the provisions of this control system in accordance with decisions of the NSC Secretariat. National Security Council Intelligence Directives (NSCIDs) have been so excepted.

16. CONTROL PROCEDURES

The following control procedures shall apply to Top Secret documents issued by NSC:

- (1) Form ~~NSC~~ 26, Signature Record and Cover Sheet will be used to indicate CIA routing of the NSC Top Secret document. Each alternate or Assistant Top Secret Control Officer who receives and/or releases the NSC Top Secret document will sign Form ~~NSC~~ 26, indicating period of custody in the left column of the form.

SECRET

SECRET

CONTROL OF NSC INFORMATION AND MATERIAL

(2) The Top Secret Control Officer initially receiving the NSC Top Secret document will:

- (a) Insure that the logging requirements applicable to all Top Secret documents are adhered to fully,
- (b) Enter the document description and registry information on Form ~~NSC~~ 26, and
- (c) Whenever a Top Secret NSC document is destroyed, the Notice of Detachment block on Form ~~NSC~~ 26 will be executed, and will be filed in the central Top Secret Control Office.

SECRET

SECRET

CHAPTER VI: CONTROL OF STAFF CRYPTOGRAPHIC INFORMATION AND MATERIAL

Par.

Page

17. HANDLING

18. CUSTODIANS

SECRET

SECRET

SECRET

CHAPTER VI: CONTROL OF STAFF CRYPTOGRAPHIC INFORMATION AND MATERIAL

17. HANDLING

Staff cryptographic information and material will be handled in accordance with the requirements and procedures of Regulations No.

25X1

and the other regulatory and instructional issuances governing the protection of cryptographic information and material. The Director of Communications is responsible for administering the transmission and control procedures for registered and unregistered cryptographic material of all classifications.

18. CUSTODIANS

Individuals specifically designated by the Director of Communications will function as the custodians of cryptographic information and material within the Agency and will be responsible to the Director of Communications for implementation of regulations and instructions governing the handling of cryptographic material.

SECRET

SECRET

CHAPTER VII

PROCEDURES FOR PROTECTION OF CLASSIFIED AND CONTROLLED INFORMATION OR MATERIAL

Par.

Page

19. STORAGE

20. TRANSMISSION

21. REPRODUCTION

22. DESTRUCTION

SECRET

SECRET

CHAPTER VII

PROCEDURES FOR PROTECTION OF CLASSIFIED INFORMATION OR MATERIAL

19. STORAGE

a. CUSTODIANS OF STORAGE EQUIPMENT

Supervisors are responsible for designating as custodians those individuals under their direct control who must have knowledge of specific safe or vault combinations. Safe combinations will be made known only to those persons who, in the course of their official duties, are required to have access thereto. It is the individual responsibility of custodians to know the proper method of locking and checking all safes to which they have access.

b. POSTING IDENTITY OF CUSTODIANS

The name, home address, and home telephone number of each custodian having access to a safe or safe-type cabinet shall be posted on the side of each drawer. Safekeeping equipment, such as vaults and other types of equipment having the lock mechanism on a door, will list the foregoing information on the inside of the door.

c. STORAGE REQUIREMENTS

(1) GENERAL

The minimum requirement for storage of classified information or material shall be a vault, safe, or fire resistant safe-type file cabinet, equipped with a built-in three-tumbler combination lock of the type approved by the Director of Security. Storage in such equipment is authorized only when the equipment is located in Agency buildings in headquarters area. Storage of such material in equipment located in non-Agency buildings

SECRET

SECRET

PROCEDURES FOR PROTECTION OF CLASSIFIED INFORMATION OR MATERIAL

or facilities in the headquarters area or in any buildings or facilities, Agency or other, outside of the headquarters area must have the specific approval of the Director of Security.

(2) STORAGE OF INFORMATION OR MATERIAL BEARING A CONTROL STAMP

Information or material which bears a control stamp such as "CIA Internal Use Only" and which is registered or classified, shall be stored in accordance with subparagraph (1) immediately above. However, information or material which is neither classified nor registered but bears a control stamp shall be kept under lock and key. If the bulk, volume, or handling of unclassified or nonregistered material bearing a control stamp presents a serious problem in the efficient operation of an office, the Director of Security should be consulted for guidance.

(3) BULK STORAGE

Bulk classified information or material may be stored in safes as required above. If the nature or bulk precludes such storage, the material shall be stored in a vault or a "secured room." The type and construction of such storage facilities must be approved in advance by the Director of Security.

(4) UNUSUAL STORAGE REQUIREMENTS

If, in unusual circumstances or for operational reasons, it is not possible to comply with the foregoing provisions, arrangements will be made, subject to the approval of the Director of Security, to safeguard the material under armed guard when such material is not in use.

SECRET

SECRET

PROCEDURES FOR PROTECTION OF CLASSIFIED INFORMATION OR MATERIAL

d. DELIVERY AND TRANSFER OF SAFES

A safe or safe-type cabinet will not be placed in use until a number has been assigned and affixed thereto by a representative of the Office of Security and the combination reset by an authorized representative of that office. When safekeeping equipment is transferred to the warehouse as surplus or to another office, the principal custodian will insure that the contents have been removed and the present combination setting is securely affixed to the outside of the safe near the combination dial. When such a safe is again placed in use, the acquiring office will call the Office of Security requesting that a new combination be set in the lock, and will not use the safe until this has been accomplished.

e. MAINTENANCE OF CLASSIFIED STORAGE EQUIPMENT

The Office of Security is responsible for the correction of mechanical defects in the operation of safekeeping equipment. It is the responsibility of the custodian to report immediately to the Office of Security when the safekeeping equipment under his care is not in proper working order.

f. COMBINATION CHANGES

Except as hereinafter provided, authorized representatives of the Office of Security are the only personnel permitted to make changes in combinations. The Director of Security may specifically authorize designated sensitive areas, offices, or staffs to exercise local control in the initial setting or changing of combinations.

SECRET

~~SECRET~~

PROCEDURES FOR PROTECTION OF CLASSIFIED INFORMATION OR MATERIAL

The combinations of all safekeeping equipment shall be changed every 12 months, on separation or transfer of custodians, when custodians no longer require access to the material contained there, or as often as good security practices require. Combinations are considered classified information and must be treated accordingly.

g. COMBINATION RECORDS

With the exception of areas, offices and staffs authorized to exercise local control over the changing and recording of combinations, as provided above, the Director of Security shall maintain a central record of the combinations of all Agency safekeeping equipment. When the combination is initially set or subsequently changed by a representative of the Office of Security, he shall maintain a record of the safe number and the combination.

25X1

20. TRANSMISSION

a. TOP SECRET INFORMATION OR MATERIAL

(1) Top Secret Control Officers

6110705036

~~SECRET~~

SECRET

PROCEDURES FOR PROTECTION OF CLASSIFIED INFORMATION OR MATERIAL

- (a) The CIA Top Secret Control Officer, Office of Central Reference, is responsible for exercising staff supervision over the transmission and control of Top Secret information or material, except that cryptographic Top Secret information or material will be handled in accordance with paragraphs 17 and 18. The duties of the CIA Top Secret Control Officer include:
- (1) Maintaining the CIA central office of record for all Top Secret information or material originated within or received by the Agency, except that, for operational reasons within the Clandestine Services, the office of record may be maintained by the Area Top Secret Control Officer, DD/P;
 - (2) Providing technical guidance and assistance to Top Secret Control personnel;
 - (3) Preparing and maintaining the CIA Top Secret Control Handbook;
 - (4) Initiating, receiving, and maintaining records of annual inventories of all Top Secret material within CIA;
 - (5) Initiating or performing periodic inspections of the Top Secret Control program;
 - (6) Maintaining current lists of Top Secret Control personnel; and
 - (7) Allocating all CIA Top Secret document-control numbers and maintaining records of them.

SECRET

PROCEDURES FOR PROTECTION OF CLASSIFIED INFORMATION OR MATERIAL

(b) Area and Unit Top Secret Control Officers will be appointed to handle the operation of the Top Secret Control program within their assigned areas.

(2) Accountability

Top Secret information or material, originated within CIA or received from non-CIA sources, will immediately be put under Top Secret Control procedures for accountability, storage, and transmission within or outside CIA. The accountability procedure will include:

(a) Numbering of Copies

Each Top Secret document and all its copies will be assigned a CIA Top Secret Control number and copy number.

(b) Permanent Registry

The CIA Top Secret Control Officer and Area and Unit Top Secret Control Officers will maintain a permanent Top Secret Control log (registry) using either Form No. 36, Top Secret Control Card, or Form No. 312, Top Secret Posting Record. The log will record the subject, CIA Top Secret Control number, copy number, receipt, routing, and disposition of all Top Secret material for which these control officers are responsible. In addition, this log, or other supporting registries under control of these officers, will show the individual having custody of any Top Secret item at any given time.

SECRET

SECRET

PROCEDURES FOR PROTECTION OF CLASSIFIED INFORMATION OR MATERIAL

(c) Document Receipt

The transfer of Top Secret information or material will be accompanied by a receipt (Form ~~455~~ 615 or Form ~~455~~ 60-122--to be redesignated Form 455--CIA Document Receipt) except when the recipient's signature on the sender's Top Secret log is substituted for the form. The document receipt will identify the addressor, addressee, and document but will contain no classified information. It will be signed by the proper recipient and returned to the sender. The name of the recipient will be printed, stamped, or typed on the form. A receipt will also be obtained if Top Secret information or material is given approved dissemination to activities outside CIA or to a foreign government.

(d) Signature Record and Cover Sheet

- (1)** Each copy of a Top Secret document retained within CIA will be covered at all times by Form ~~455~~ 26, Signature Record and Cover Sheet, which must be signed by each person who reads the document or sees any part of its contents. Form ~~455~~ 26 will also be attached to non-CIA Top Secret material when received. However, individuals who routinely handle Top Secret material within message centers, or communications-center personnel who administratively handle a large volume of such information daily, will not be required

SECRET

SECRET

PROCEDURES FOR PROTECTION OF CLASSIFIED INFORMATION OR MATERIAL

to sign Form ~~26~~ 26 when such personnel are identified by roster as having had access to Top Secret information on a given date.

- (2) Each copy of a National Security Council Top Secret document in CIA will be covered at all times by Form ~~26~~ 26.

(e) Change-of-Duty Status

Upon change-of-duty assignment, or upon separation from the Agency, each individual, prior to his departure, will properly account to his successor or other appropriate authority for all Top Secret information or material for which he is custodian.

(f) Annual Inventories

Each Operating Official, ^{005 07} on or about 1 April of each year, will make a physical inventory of all Top Secret information or material held in custody within his jurisdiction. The inventory report will be forwarded to the CIA Top Secret Control Officer. For inventory purposes, a document is deemed to have been accounted for if:

- (1) It is physically located, or
- (2) A receipt for it is held from another office of record, or
- (3) A destruction certificate is held for the document.

(g) Lost-and-Found Top Secret Information or Material

Lost-and-found Top Secret information or material will be reported immediately to the Director of Security for investigation and to the CIA Top Secret Control Officer.

SECRET

SECRET

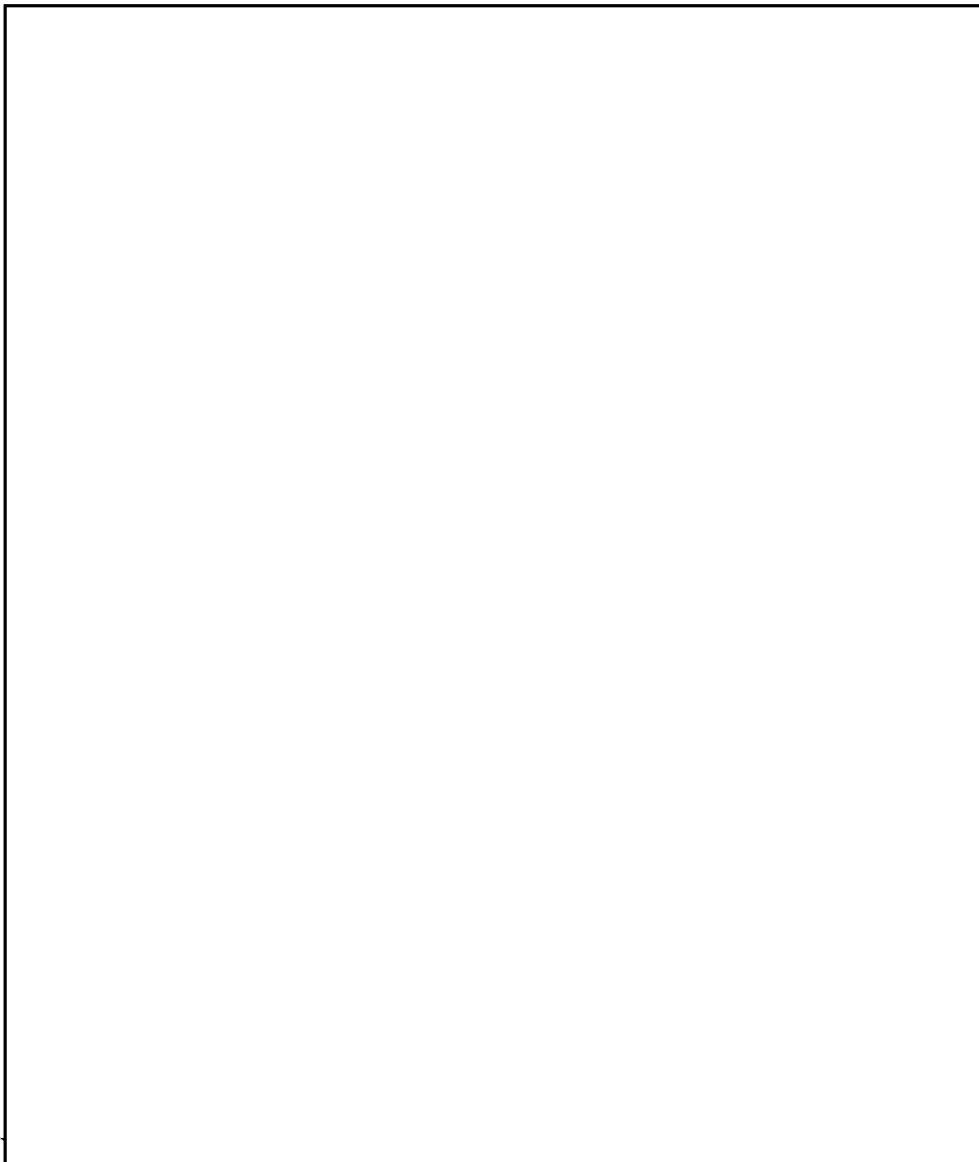
PROCEDURES FOR PROTECTION OF CLASSIFIED INFORMATION OR MATERIAL

(3) Transmission

(a) Preparation for Transmission

Unless hand-carried by the custodian or transmitted by CIA-approved electrical means, Top Secret information or material will be prepared for transmission as follows:

(1) Within the Continental United States:



25X1

SECRET

~~SECRET~~

PROCEDURES FOR PROTECTION OF CLASSIFIED INFORMATION OR MATERIAL

25X1



FMB

(2) Outside the Continental United States:

For transmission outside the continental United States,
prepare in accordance with CIA Regulation

25X1

(b) Methods of Transmission

Under no circumstances will Top Secret information or material
be transmitted by mail, registered or otherwise, or by express.
Transmission will be by one of the methods listed below:

(1) Within the Continental United States:

- (a) By couriers of the Office of Logistics, or
- (b) By the Office of Security when special handling
is required, or
- (c) By Top Secret Control personnel, or
- (d) By custodians of Top Secret material, or
- (e) By CIA-approved electrical means, or
- (f) By Armed Forces courier service.

(2) Outside Continental United States:

~~SECRET~~

~~SECRET~~

SECRET

PROCEDURES FOR PROTECTION OF CLASSIFIED INFORMATION OR MATERIAL

(a) By channels established in accordance with CIA Regulation

25X1

(b) By CIA-approved electrical means, or

(c) By the Office of Security, in unusual cases where special handling is required. Armed escorts may be provided for the protection of bulk shipments or extremely sensitive material when deemed necessary.

(See Regulation)

25X1

b. SECRET AND CONFIDENTIAL INFORMATION OR MATERIAL

(1) ACCOUNTABILITY

Operating Officials will prescribe measures within their jurisdiction to properly control at all times the dissemination of Secret and Confidential information and material. Such measures will include keeping good accountability records (Logs) and severely limiting the number of documents originated as well as the number of copies reproduced. Accountability records will include logs kept on Secret and Confidential information or material at the initial point of receipt and at the final point of dispatch in an Office, Operating Division, or Senior staff, and within the Office of the Director, as approved by the Executive Officer. This handbook is not to be construed as preventing Operating Officials from instituting other logs where deemed advisable.

31107010045

SECRET

SECRET

PROCEDURES FOR PROTECTION OF CLASSIFIED INFORMATION OR MATERIAL

(2) TRANSMISSION

(a) Preparation for Transmission

(1) Within Headquarters

- (a) Properly sealed chain or single envelopes, no further cover required, may be used by authorized persons.
- (b) Preparation in accordance with paragraph 20 a. (3) above may be substituted for the chain envelope if the sender deems such precaution advisable.

(2) Outside Headquarters

Secret and Confidential information or material to be transmitted outside headquarters, unless hand-carried by the custodian, will be double-wrapped and addressed in accordance with paragraph 20 a. (3) above. Control designations on the inner envelope or wrapper, "To be opened by the addressee only" or "To be opened by (specific individual or activity) only," are optional. When courier service is used, Form ~~240-4~~ 240-4, Courier's Classified Mail Receipt, will be prepared in duplicate, and attached to the outer envelope or cover.

(b) Methods of Transmission

Secret and Confidential information or material, except cryptographic, will be transmitted by one of the methods indicated below:

SECRET

SECRET

PROCEDURES FOR PROTECTION OF CLASSIFIED INFORMATION OR MATERIAL

- (1) By one of the methods authorized for Top Secret; or
- (2) By an authorized CIA courier; or
- (3) By U. S. Post Office registered mail; or
- (4) By U. S. Post Office registered mail through Army, Navy, or Air Force postal facilities, provided material does not at any time pass out of U. S. Government control and through a foreign postal system

25X1

(5)

- (6) By messenger for delivery within CIA buildings or to other Agency-occupied buildings in the same vicinity; or
- (7) By armed escorts who may be provided for the protection of bulk shipments or extremely sensitive material when deemed necessary (see Regulation or
- (8) By any other means specifically approved by the Director of Security.

25X1

(c) Document Receipts

Documents receipts will be signed by the proper recipient and returned to the sender.

- (1) Within Headquarters

611080100

SECRET

~~SECRET~~

PROCEDURES FOR PROTECTION OF CLASSIFIED INFORMATION OR MATERIAL

The transfer by Form 615 of Secret and Confidential material is optional with the sender. The recipient's signature in the sender's log may be substituted for this form when a receipt is required by the sender.

(2) Outside Headquarters

The transfer of Secret material will be by Form 615. Receipt for Confidential material is optional with the sender.

c. REGISTERED DOCUMENTS

(1) DEFINITIONS

- (a) A "registered document" is a classified document bearing a short title and registered number, which is marked "Registered Document," and for which periodic inventory is established.
- (b) A "registered number" is the number assigned to each copy of a registered document for accounting purposes. A serially numbered document is not necessarily a registered document.
- (c) The "office of record" is the office that establishes and maintains accountability for a particular registered document and to which reports of inventory, transfer, and destruction are sent. The office of record is not necessarily the office of origin nor the office of issue of the document involved.

~~SECRET~~

~~SECRET~~

PROCEDURES FOR PROTECTION OF CLASSIFIED INFORMATION OR MATERIAL

- (d) The "office of origin" is the office responsible for the content and correct preparation of a registered document.
- (e) A "long title" is the descriptive name assigned a specific document by the office of origin.
- (f) A "short title" is a brief, unclassified, identifying combination of letters and/or numbers assigned to a specific registered document for security purposes. A short title must never reveal subject content.
- (g) A "witnessing officer" is the officer who observes and verifies the inventory or destruction of registered documents.

(2) AUTHORITY TO REGISTER

Operating Officials, when they deem registered control is necessary for security reasons, may register any classified material, documents, and devices that they are authorized to classify.

(3) CIA CUSTODIAN OF REGISTERED DOCUMENTS

The CIA Custodian of Registered Documents (the CIA Top Secret Control Officer, OCR) serves as the office of record for registered documents originated within, or received by, the Agency. However, for operational reasons within the Clandestine Services, the office of record may be the DD/P Custodian of Registered Documents.

(4) REFERENCES TO REGISTERED DOCUMENTS

- (a) All references to registered documents or devices made in reports of possession, transfer certificates, reports of

211773259

~~SECRET~~

SECRET

PROCEDURES FOR PROTECTION OF CLASSIFIED INFORMATION OR MATERIAL

destruction, or unclassified documents or correspondence will be by registered number, date, and short title only. Such reports or correspondence will not be classified. If a short title is used, every symbol of that title will be included.

- (b) A document that includes both the short and long titles of a registered document will be given the same classification as the registered document itself.

(5) ACCOUNTABILITY

Registered material, upon origination or reproduction within CIA or upon receipt from non-CIA sources, will be put immediately under control of the appropriate office of record for accountability. The accountability procedure will include:

(a) Permanent Registry

The CIA and Area custodians of registered documents will maintain a permanent log on Form ~~W~~ 303, Registered Material Transfer Certificate and Semi-annual Report, of all registered documents for which they are responsible. These registries will show the person accountable for registered material at any given time.

(b) Form ~~W~~ 303

Form ~~W~~ 303 will be used for receipt, transfer, and semi-annual reporting of registered documents.

SECRET

SECRET

PROCEDURES FOR PROTECTION OF CLASSIFIED INFORMATION OR MATERIAL

(c) Inventories

(1) Originated Within CIA:

The CIA offices of record will make, on or about 1 April and 1 October of each year, a semi-annual inventory of all CIA-produced registered documents within their control.

(2) Originated Outside CIA:

CIA offices of record will comply strictly with the inventory instructions contained in non-CIA-originated documents or as required by the non-CIA registered document office of record.

(d) Lost-and-Found Registered Documents

Lost-and-found registered documents will be reported immediately to the Director of Security for investigation and to the appropriate CIA office of record.

(6) MARKING

In addition to the marking required for classified documents, each registered document will be marked conspicuously "Registered Document" and will be assigned a long title, short title, and registered number. Each registered document will contain a title page, or a registered-document cover sheet will be permanently attached. If a registered document consists of more than one volume, each volume will bear a separate short title. Reprints (additional copies) will retain the exact short title of the original.

SECRET

SECRET

PROCEDURES FOR PROTECTION OF CLASSIFIED INFORMATION OR MATERIAL

(7) TRANSMISSION

(a) Preparation for Transmission

Registered documents will be prepared for transmission in accordance with paragraph 20 a. (3) above.

25X1

(b) Transmission Procedure

Registered documents will be transmitted in accordance with the methods prescribed for their security classification.

(c) Cables

(1) Cables originating within CIA will be transmitted and controlled in conformity to the security principles of continuous accountability and control as outlined in Regulation

25X1

25X1

(2) Cables originating outside CIA will be transmitted and controlled in accordance with the provision of Regulation

(d) Custodianship by Individuals in Traveling Status

An individual in a traveling status who is authorized to have in his possession classified information or material will safeguard such material by the following methods:

31270 5200

SECRET

SECRET

PROCEDURES FOR PROTECTION OF CLASSIFIED INFORMATION OR MATERIAL

- (1) By keeping the material under his personal, physical control at all times. It is the responsibility of personnel carrying classified material to use proper judgment in their actions so that they do not place themselves in situations where the material could be compromised.
- (2) By not carrying classified material across international borders where such material might be liable to scrutiny by customs inspectors or other unauthorized individuals. Such material should be sent in advance by an approved method of transmission.

21. REPRODUCTION

a. TOP SECRET INFORMATION AND MATERIAL

All reproduced Top Secret information and material will be placed immediately under the Top Secret Control procedures as outlined in paragraph 20 a. (2) above.

(1) Material Originated Within CIA

Authorization to copy, extract from, or reproduce Top Secret material originated within CIA will be obtained from the office of origin.

(2) Information or Material Originated Outside CIA

Authorization to copy, extract from, or reproduce non-CIA Top Secret information or material will be obtained from the

SECRET

SECRET

~~SECRET~~

PROCEDURES FOR PROTECTION OF CLASSIFIED INFORMATION OR MATERIAL

originating Government agency or department when possible. Such authorization will be obtained through the Office of Central Reference, except that, for operational reasons, authorization may be sought directly by the Office of the Deputy Director (Plans). When the Agency needs to reproduce non-CIA material for internal use and it is not possible to secure authorization within the time available, limited reproduction of the material may be made, provided each copy is plainly marked: "This copy has been reproduced to meet the internal needs of CIA. It must not be released or shown to any person outside CIA."

b. SECRET AND CONFIDENTIAL INFORMATION OR MATERIAL

(1) Originated Within CIA

Copying, extracting from, or reproducing Secret and Confidential information or material originated within CIA is authorized on a limited basis to meet Agency needs. However, any restrictions imposed by the originating office will be honored.

(2) Originated Outside CIA

(a) Non-CIA Secret and Confidential information or material may be reproduced for the purpose of central processing without consent of the originating agency or department as CIA needs require. However, any restrictions imposed by the originating agency or department will be honored.

(b) Reproduction may be performed for another member agency if the intelligence or information was originally given

SECRET

~~SECRET~~

SECRET

PROCEDURES FOR PROTECTION OF CLASSIFIED INFORMATION AND MATERIAL

general distribution to all IAC member agencies, or ^{was} ~~were~~
otherwise made generally available to ^{them} ~~allies~~.

22. DESTRUCTION

a. DEFINITIONS

(1) Destruction

"Destruction" of information or material is the physical act of reducing such material to a condition beyond recognition and reconstruction.

(2) Burn Teams

Two or more persons designated by an Operating Official on either a temporary or a permanent basis, for the purpose of accomplishing the destruction of classified information or material constitute a "burn team."

(3) Accountable Material

"Accountable information or material" is any classified information or material which bears specific instructions requiring accountability to the originator.

(4) Registered Information or Material

"Registered information or material" is any classified information or material bearing a short title and registered number, which is marked "Registered Document," and for which periodic inventory is established.

(5) Record Information or Material

55

811970000

SECRET

~~SECRET~~

PROCEDURES FOR PROTECTION OF CLASSIFIED INFORMATION OR MATERIAL

"Records," as defined in Sec. 366 of the Records Disposal Act of July 7, 1943, (44 U.S.C. 366-380) as amended, (57 Stat. 380) includes: "All books, papers, maps, photographs, films, recording equipment, or other documentary materials, regardless of physical form or characteristics, made or received by any part of any agency of the U. S. Government in pursuance of Federal law or in connection with the transaction of public business, and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the government, because of the informational value of data contained therein."

(6) Nonrecord Information or Material

"Nonrecord information or material" consists of library and museum material made or acquired and preserved solely for reference or exhibition purposes, extra copies preserved only for convenience of reference, and stocks of publications or processed documents.

(7) Cryptographic Information or Material

"Cryptographic information or material" includes all cryptographic system equipment, devices, communications cover techniques, and associated instructional documents employed in, or pertinent to, the encryption and decryption of staff communications between headquarters and field installations, or between field installations.

~~SECRET~~

SECRET

PROCEDURES FOR PROTECTION OF CLASSIFIED INFORMATION OR MATERIAL

(8) Classified Waste

"Classified waste" includes, but is not limited to, notes, preliminary drafts, copies, carbons, stencils, worksheets, blank paper containing impressions from classified writing, once-used typewriter ribbons, devices used to activate automatic typing machines, dictaphone recordings, plates, exposed films (developed or undeveloped), and printed masters common to printing and reproduction operations.

(9) Records Control Schedule

A "records control schedule" is an approved, written plan identifying material that is to be retained or destroyed.

(10) Office of Record

The "office of record" is the office which establishes and maintains accountability for a particular registered document and to which reports of inventory, transfer, and destruction are sent. The office of record is not necessarily the office of origin, or the office of issue of the document involved.

b. METHODS

- (1) Subject to the procedures of paragraph c. below, all classified information or material, including classified waste, or that which bears a control stamp, will be destroyed by burning or by such other method as may be approved by the Director of Security. All such information or material to be destroyed will be torn or shredded into small pieces in preparation for disposal.

PROCEDURES FOR PROTECTION OF CLASSIFIED INFORMATION OR MATERIAL

c. PROCEDURES

(1) Record and Certificate of Destruction

Operating Officials will institute appropriate accountability records to reflect the destruction of Secret and Confidential information and material. Such accountability records will be retained by the Agency for a period of three years, after which they may be destroyed. A certificate of destruction is not necessary unless the information or material bears a specific accountability requirement.

(2) Classified waste, except "Restricted Data" waste - see paragraph

(3) below, will be placed in receptacles conspicuously marked "Secret," and appropriately safeguarded until destroyed.

(3) "Restricted Data"

(a) All "Restricted Data" intended for destruction shall be transmitted by "Q"-cleared courier to the OCR Restricted Data Control Point, which shall be responsible for the destruction.

(b) "Restricted Data" may be destroyed only by persons authorized to have access thereto. Personal notes and other "Restricted Data" waste may be destroyed by a "Q"-cleared person (or Military personnel certified for access thereto) without transmittal to the OCR "Restricted Data" Control Point if facilities approved by the Director of Security for destruction are available.

PROCEDURES FOR PROTECTION OF CLASSIFIED INFORMATION OR MATERIAL

(4) Cryptographic Information and Material

All cryptographic information and material will be destroyed pursuant to instructions issued by the Director of Communications and in accordance with the policies prescribed in this Manual.

(5) Registered Information and Material

Noncryptographic registered information or material will be forwarded to the Area Custodian of Registered Documents for disposition or destruction.

(6) Top Secret Information or Material

(a) CIA Top Secret Information or Material

- (1) Top Secret information or material (except Top Secret waste - see paragraph 22.b.) to be destroyed will not be placed in "Secret Classified Waste" receptacles. Destruction will be accomplished by the appropriate Top Secret Officer or his designee in the presence of a witnessing CIA official having a Top Secret Clearance. Destruction will be in the manner prescribed in paragraph 22. b. (1) above.

(2) Records

When a Top Secret document is destroyed, the Notice of Detachment block of Form ~~NY~~ 26, Signature Record and Cover Sheet, will be executed. Form ~~NY~~ 26 will

PROCEDURES FOR PROTECTION OF CLASSIFIED INFORMATION OR MATERIAL

then be forwarded to the appropriate Top Secret office of record, which will make proper entries in the Top Secret log or Registry.

(b) Non-CIA Top Secret Information or Material

Top Secret information or material originated by another department or Government agency will not be destroyed except upon authorization from the CIA Central Top Secret Control Office or, within the DD/P Component, from the Area Top Secret Control Officer.

(7) Technical, Mechanical, or Electrical Devices (Excluding Cryptographic Material)

The classified components will be removed from such devices and will be destroyed by burning or mutilation in the presence of a witnessing CIA official. If removal of the classified components from such devices is not practicable, the entire item will be destroyed by burning or mutilation or by a method equally complete.

(8) Accountable Information or Material

When accountability is required by the originator, a certificate of destruction will be executed in duplicate and will be signed by the individual authorizing destruction, the person accomplishing destruction, and the witnessing CIA official, and will bear the date of destruction and exact identity of the material. The original will be forwarded to the originator, and the duplicate will be retained for one year by the office authorizing destruction.

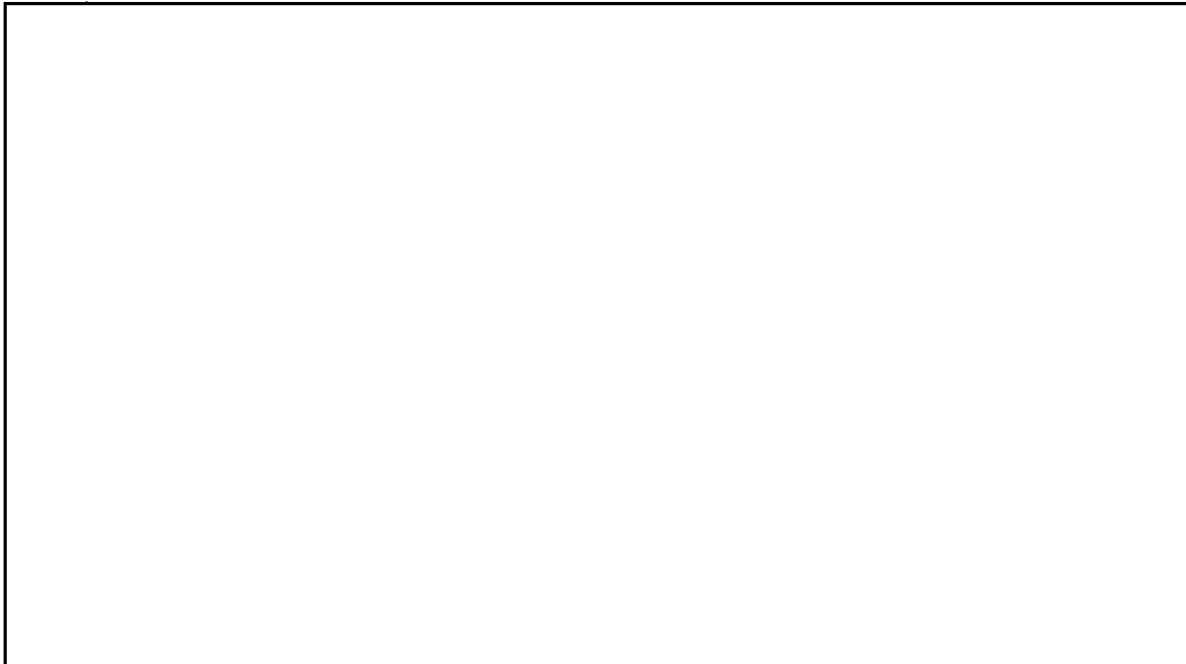
SECRET

CHAPTER VIII: CONTROL OF SEC RESTRICTED DATA

Par.

Page

23. DEFINITION



SECRET

SECRET

CHAPTER VIII: CONTROL OF AEC RESTRICTED DATA

23. DEFINITION

- (1) The term "Restricted Data" means all data concerning (1) design, manufacture, or utilization of atomic weapons; (2) the production of special nuclear material; or (3) the use of special nuclear material in the production of energy, but shall not include data declassified or removed from the Restricted Data category pursuant to Section 112 of the Atomic Energy Act of 1954. It includes data both on the atomic energy program of the United States, and on the programs of the United Kingdom and Canada, with whom the United States has formal agreements under the said Act; it will include also the program of any other nation with whom the United States might enter into similar formal agreement. It does not include unevaluated or evaluated information or intelligence concerning the atomic energy programs of other nations which has been removed from the Restricted Data category upon joint determination by the Atomic Energy Commission and the Director of Central Intelligence as necessary to the functions of CIA, in accordance with Section 112e of the Atomic Energy Act of 1954.
- (2) The term "Formerly Restricted Data" designates material removed from the Restricted Data category pursuant to Section 112d of the Atomic Energy Act of 1954, in accordance with a joint determination by the Atomic Energy Commission and the Department of Defense that the data relates primarily to the military utilization of atomic weapons and can be adequately safeguarded as defense information.

SECRET

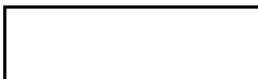
25X2

Approved For Release 2006/04/13 : CIA-RDP70-00211R000900210002-6

Next 6 Page(s) In Document Exempt

Approved For Release 2006/04/13 : CIA-RDP70-00211R000900210002-6

SECRET

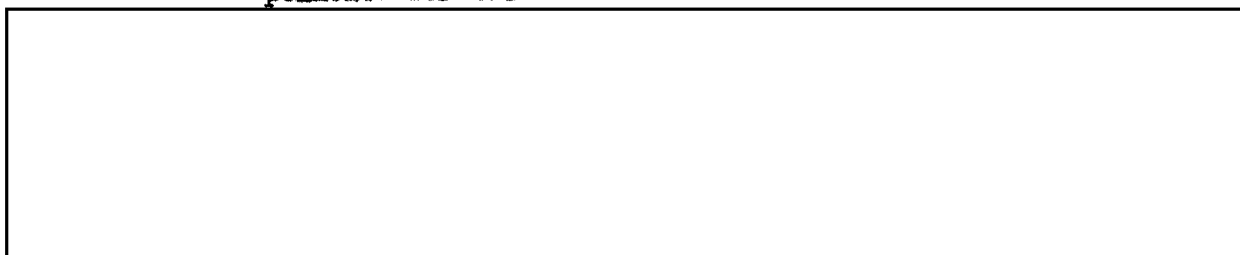


SECURITY

25X1

SECURITY OF INFORMATION AND MATERIAL

SYNOPSIS: This regulation provides for the security of official data and classified information and material entering or leaving the Agency and prescribes policies for the control of such material.



25X1

CONTENTS

	<i>Page</i>
Care and Use of Official Data	
Classification of Official Information and Material	
Control-Stamping of Information and Material	
Control of Personnel-Security Files	
Control of NSC Information and Material	
Control of Staff Cryptographic Information and Material	
Policies for the Protection of Classified Information and Material	
Control of AEC Restricted Data	

1. CARE AND USE OF OFFICIAL DATA

a. GENERAL

All information and material, classified or unclassified, received or compiled by the Central Intelligence Agency is "official data" and is the property of the U. S. Government. The restrictions and prohibitions provided in this regulation apply not only to all intelligence information or material, but also to any statistical, administrative,

SECRET

SECRET[REDACTED]
SECURITY

25X1

or general information or material, regardless of the fact that it may already be a matter of public record. These restrictions and prohibitions apply also to all official data used, or compiled by CIA, and obtained from outside sources, public or private. Termination of employment in the Agency will not affect employee responsibility under this regulation.

b. POLICY

(1) Official data, classified or unclassified, will be used only in the performance of CIA official business, and will not be copied or removed from the files of the Agency for release outside of CIA except by officials so authorized by the Director of Central Intelligence.

(2) The accumulation of copies of documents containing official data, classified or unclassified, for inclusion in a personal file, and the appropriation of such material for personal use or benefit is prohibited. Unclassified employment documents and similar personal official documents are excepted, under the provisions of this regulation.

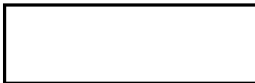
(3) STATUTORY REQUIREMENTS

The principles governing the care and use of classified official data and the penalties prescribed for violations of these principles are set forth in Public Law 99, 83rd Congress (18 U.S.C. 793 and 794). Pertinent extracts from the United States Code will be found in Chapter I [REDACTED]

25X1

SECRET


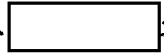
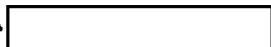
SECRET



SECURITY

25X1

c. RESPONSIBILITIES

- (1) The Director of Personnel is responsible for insuring that all personnel processed through the Office of Personnel shall report to the Office of Security to read and become familiar with the appropriate provisions of this Regulation before entrance on duty or separation from the Agency. Principal officers of  field installations are responsible for insuring that all  field personnel not processed through headquarters and entering on duty or being separated from the Agency read and become familiar with these requirements.
- (2) Any representative of CIA who is authorized by competent authority to negotiate with individuals or organizations for services shall insure that the appropriate provisions of this regulation are incorporated in the Secrecy Agreement or contract. These provisions may be incorporated by reference where feasible. (See paragraph 7 of 

25X1

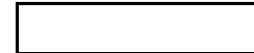
2. CLASSIFICATION OF OFFICIAL INFORMATION AND MATERIAL

a. GENERAL

The accomplishment of the CIA mission depends upon the degree to which official information and material regarding every function, action, method, and technique of the Agency is protected successfully from disclosure to unauthorized persons. Maximum protection of such information and material requires not only prevention of

SECRET

SECRET

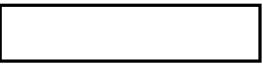


SECURITY

25X1

penetration of the Agency and disclosure of information or material outside the Agency, but also requires that there be internal protection to limit the disclosure of information or material within the Agency to those individuals whose duties require access to it.

b. CLASSIFICATION POLICY

(1) Information or material which requires protection in the interests of national defense shall be limited to three categories of classification, which in descending order of importance shall carry one of the following designations: Top Secret, Secret or Confidential. (See paragraph 6 of ) Such information and material shall not be given a higher classification than is justifiable on the basis of content. The classification category shall be determined by the degree of secrecy warranted for the control of the information or material in terms of the potential effect its disclosure might have on the defense of the nation, or on the intelligence efforts of the United States Government, and not upon the mere desirability of restricting access under the need-to-know principle.

25X1

(2) Authority to assign an original classification to information or material shall be delegated to officials and employees throughout the Agency as necessary to the orderly and expeditious transaction of Agency business. No person other than one to whom such authority has been delegated shall assign an original classification.

SECRET

SECRET

25X1

SECURITY

- (3) Classified information or material shall be reviewed on a continuing basis to determine the current appropriateness of the classification assigned with a view to declassification or reclassification when appropriate.

c. **RESPONSIBILITIES**

- (1) The Assistant Director for Central Reference shall establish a CIA Classification Control System which will provide for the control of the classification and reclassification of information and material.
- (2) The CIA Classification Control Officer, under the Assistant Director for Central Reference, is responsible for the establishment and issuance of procedures governing the Agency Classification Control System. These procedures shall be developed and coordinated with Assistant Classification Control Officers.
- (3) The CIA Classification Control Officer, in collaboration with the Directors of Training and Security, shall develop such training materials and programs as necessary or desirable to provide for the proper performance of classification-control functions.
- (4) Assistant Classification Control Officers are responsible for the administration of the Classification Control System within their area of responsibility in accordance with this regulation and such implementing procedures as are developed by the CIA Classification Control Officer, including continuing review and inspection of the classification and declassification

SECRET

SECRET

25X1

SECURITY

procedures. These officers are also responsible for maintaining records of those persons who have been designated as Authorized Classifiers.

- (5) Authorized Classifiers, Assistant Classification Control Officers, and the CIA Classification Control Officer are the only persons authorized to apply an original classification to information or material. Authorized Classifiers are responsible for the proper original classification of information and material.
- (6) The CIA Classification Control Officer and Assistant Classification Control Officers shall collaborate with the Director of Security in the establishment of an inspection program that will insure that the provisions of this regulation are properly applied.

d. DEFINITIONS

Information and material shall be classified in accordance with the definitions of classification categories set forth in paragraph 6 of

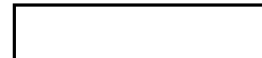
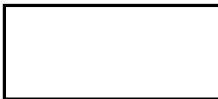
3. CONTROL-STAMPING OF INFORMATION AND MATERIAL

Control stamps, which are not to be construed as a classification, may be used only whenever it is necessary to protect sources and methods by indicating to authorized recipients a specific limitation in the handling of the information or material. Procedures for the use of control stamps are prescribed in paragraph 10 of

25X1

SECRET

SECRET



25X1

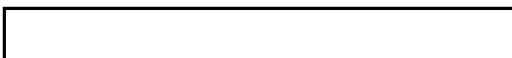
SECURITY

4. CONTROL OF PERSONNEL-SECURITY FILES

a. AUTHORITY

Personnel Security files will be controlled and safeguarded, to protect the confidential character and sources of information contained therein, in the interest of our national security and welfare and the protection of government personnel against unfounded or disapproved allegations, in accordance with the policy contained in the Presidential Memorandum to All Officers and Employees in the Executive Branch of the Government dated 13 March 1948, and section 9 (c) of Executive Order 10450 dated April 27, 1953.

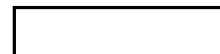
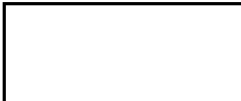
b. POLICY

- (1) Prior authorization by the Director of Central Intelligence is required for the release of personnel-security files or information contained therein to persons or activities outside of this Agency with one exception: investigative information (see  which is contained in the personnel security files of the Agency may be released by the Director of Security to accredited representatives of other agencies and departments of the executive branch of the Government.
- (2) Any subpoena, demand, or request for personnel-security files or information contained therein which is received by any

25X1

SECRET

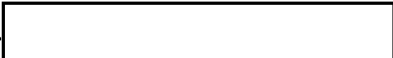
SECRET



SECURITY

25X1

employee of the Agency and which does not fall within the provisions of this regulation, shall be referred without delay to the Director of Security and the General Counsel, ^{and they} ~~who~~ will make appropriate recommendation to the Director of Central Intelligence.

- (3) The personnel-security files of the Agency will not be released to any Agency official except with the approval of the Director of Central Intelligence. This restriction does not apply to officials connected with the processing of a case under the provisions of Regulation  The Director of Security or the Deputy Director of Security may release personnel-security files to these officials for use in adjudication of the case.

25X1

- (4) The Director of Security, at his discretion, may release pertinent personnel-security information to Deputy Directors and Operating Officials of the Agency for reasons involving administration or personnel actions and problems related thereto. In any release of personnel security information the Director of Security will be guided by the need to preserve the confidential character and sources of information. It will be incumbent upon the Deputy Directors and Operating Officials to preserve inviolate the confidential character of personnel-security information.

c. RESPONSIBILITY

The Director of Security is responsible for the appropriate classification, control, and protection of the personnel-security files of the Agency to prevent unauthorized access thereto.

8
SECRET

SECRET

25X1

SECURITY

d. PROCEDURES

Procedures for release of personnel-security information are prescribed in paragraph 14 of [REDACTED]

5. CONTROL OF NATIONAL SECURITY COUNCIL INFORMATION OR MATERIAL

a. POLICY

- (1) In the interest of national security, the highest degree of protection shall be applied to the control of all classified National Security Council information or material.
- (2) Employees and officials of CIA who have access to classified NSC information or material are authorized to disclose it only when the need-to-know principle is paramount.

b. RESPONSIBILITIES

- (1) Agency employees and officials who originate or receive NSC classified information or material are responsible for preventing any unauthorized disclosure.
- (2) CIA employees and officials authorized to disclose NSC classified information or material are responsible for advising the recipient that such information or material is involved and for issuing appropriate precautionary instructions to prevent its disclosure to any persons except those required to have access to it.

c. PROCEDURES

Special Agency procedures for the control and handling of Top Secret information or material issued by the NSC are set forth in paragraph

15 [REDACTED]

SECRET

SECRET





25X1

6. CONTROL OF STAFF CRYPTOGRAPHIC INFORMATION AND MATERIAL

a. POLICY

25X1

Staff cryptographic information and material will be handled in accordance with the requirements and procedures of Regulation 
Regulation  and the other regulatory and instructional issuances governing the protection of cryptographic information and material.

b. RESPONSIBILITIES

- (1) The Director of Communications is responsible for administering the transmission and control procedures for registered and unregistered cryptographic information and material of all classifications.
- (2) Individuals specifically designated by the Director of Communications will function as the custodian of staff cryptographic information and material within the Agency and will be responsible to the Director of Communications for implementation of the regulations and instructions referred to in paragraph 6a above.

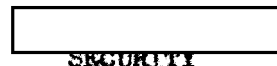
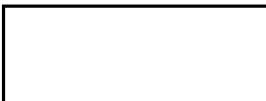
7. POLICIES FOR PROTECTION OF CLASSIFIED INFORMATION AND MATERIAL

Classified information and material shall be protected in accordance with the following policies:

a. STORAGE

- (1) The Director of Security is responsible for establishing the requirements for storage of classified information or material.

SECRET

SECRET

25X1

The minimum requirements for such storage shall be a vault, safe, or fire-resistant safe-type file cabinet, equipped with a built-in three-tumbler combination lock of the type approved by the Director of Security. Storage in such equipment is authorized only when the equipment is located in Agency buildings in headquarters area. Storage of such material in equipment located in non-Agency buildings or facilities in the headquarters area or in any buildings or facilities, Agency or otherwise, outside of the headquarters area must have the specific approval of the Director of Security.

- (2) Information or material which bears a control stamp such as "CIA Internal Use Only" and which is also registered or classified, shall be stored in accordance with subparagraph (1) immediately above. However, information or material which is neither classified nor registered but bears a control stamp shall be kept under lock and key. If the bulk, volume, or handling of unclassified or nonregistered information or material bearing a control stamp presents a serious problem in the efficient operation of an office, the Director of Security should be consulted for guidance.
- (3) Safes, vaults, safekeeping devices, other storage equipment, or secure areas shall not be purchased, constructed, or contracted for until the specifications of the equipment have been

11

SECRET

25X1

SECURITY

approved by the Director of Security in coordination with the Director of Logistics and the Operating Official concerned. This policy shall also apply when classified or controlled material are to be stored in warehouses or other structures.

b. TRANSMISSION

- (1) Proper methods of transmission of classified information or material shall be maintained at all times to insure adequate protection. Proper methods include keeping good accountability records, as well as limiting the number of classified documents or items that are originated or reproduced. The number of copies of classified documents shall be kept to a minimum to decrease the risk of compromise and to relieve the financial burden on the Government in protecting such information or material.
- (2) The custodian of classified information or material is responsible for its safekeeping and determining the identity, security clearance, and need to know of the proposed recipient prior to the physical release or disclosure.
- (3) The requirements and procedures governing the transmission and control of such information and material are prescribed in paragraph 20 of [REDACTED]

c. REPRODUCTION

- (1) Reproduction of classified information or material is authorized as specified in paragraph 21 of [REDACTED] in order to meet the internal needs of CIA; however, severe limitations should be imposed on the number of documents or items reproduced.

d. DESTRUCTION

[REDACTED]
SECURITY

25X1

- (1) Classified information and material, or that which bears a control stamp, originated in or received by the Agency will be destroyed in the presence of an authorized CIA official. Destruction will be by burning or by other methods authorized by the Director of Security. Such information or material, including classified waste, must be continuously protected from unauthorized access until completely destroyed. Operating Officials may designate "burn teams" when certificates of destruction are required, or when the custodians of sensitive information or material determine that it should not be deposited at "classified waste" depositories.
- (2) Documentary record information or material, made or received by the Agency in connection with transactions of official business and preserved as evidence ^{of} ~~by the~~ organization, functions, policies, operations, decisions, or procedures may be destroyed only in accordance with the act of July 7, 1943, c. 192, 57 Stat. 380, as amended, 44 U.S.C. 366-380. This policy will be implemented in accordance with approved Agency Records Control Schedules. In the event such schedules have not been prepared, questions as to whether the material is Record or Nonrecord should be referred to the CIA Records Officer or appropriate Area Records Officer.
- (3) Non-record classified information or material, consisting of extra copies and duplicates including shorthand notes, preliminary drafts, used carbon paper, and other information or material of similar temporary nature, may be destroyed upon authorization of the Custodian as soon as it has served its purpose. (See paragraph 22 of [REDACTED])

25X1

~~SECRET~~

25X1

SECURITY

8. CONTROL OF ATOMIC ENERGY COMMISSION "RESTRICTED DATA"

a. DEFINITION

- (1) The term "Restricted Data" means all data concerning (1) design, manufacture, or utilization of atomic weapons; (2) the production of special nuclear material; or (3) the use of special nuclear material in the production of energy, but shall not include data declassified or removed from the Restricted Data category pursuant to Section 142 of the Atomic Energy Act of 1954. It includes data both on the atomic energy program of the United States, and on the programs of the United Kingdom and Canada, with whom the United States has formal agreements under the said Act; it will include also the program of any other nation with whom the United States might enter into similar formal agreement. It does not include unevaluated or evaluated information or intelligence concerning the atomic energy programs of other nations which has been removed from the Restricted Data category upon joint determination by the Atomic Energy Commission and the Director of Central Intelligence as necessary to the functions of CIA, in accordance with Section 142e of the Atomic Energy Act of 1954.
- (2) The term "Formerly Restricted Data" designates material removed from the Restricted Data category pursuant to Section 142d of the Atomic Energy Act of 1954, in accordance with a joint determination by the Atomic Energy Commission and the Department of Defense that the data relates primarily to the military utilization of atomic weapons and

~~SECRET~~

25X2

Approved For Release 2006/04/13 : CIA-RDP70-00211R000900210002-6

Next 5 Page(s) In Document Exempt

Approved For Release 2006/04/13 : CIA-RDP70-00211R000900210002-6

~~SECRET~~



25X1

~~SECURITY~~

d. PROCEDURES

Procedures for the receipt, handling, transmission, storage, protection,
and destruction of Restricted Data are set forth in Chapter VIII of



0000000000

21

~~SECRET~~

CONTROL OF AEC RESTRICTED DATA

concurrence or to the Intelligence Advisory Committee through the Joint Atomic Energy Intelligence Committee if the information involved falls under the purview of DCID 11/1.